DETAILED ACTION

Response to Arguments

1. Applicant's arguments see pages 12 – 16, filed 11/30/2007, in view of Examiner's amendments to the claims 1-2, 4-12, 14-16, 18, 20-27, 29-35 and 59 have been fully considered and are persuasive.

Allowable Subject Matter

2. Claims 1-2, 4-12, 14-16, 18, 20-27, 29-35 and 59 are allowed. Claims have been renumbered as 1-32.

3. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Michael L. Drapkin, registration number 55,127 on June 26, 2008.

IN THE CLAIMS:

1. (Amended) A method of establishing a secure communication link between a smart card and a central computer system through a communication network, the method comprising the steps of:

receiving at a smart card communication device an outgoing secure radio frequency signal transmitted from the smart card, the secure radio frequency signal including secured data formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission beginning at the smart card and extending to the central computer system;

demodulating the outgoing secure radio frequency signal using the smart card communication device to produce an outgoing secure data signal, wherein the demodulating of the outgoing secure radio frequency signal is without deciphering the secured data;

formatting the outgoing secure data signal in accordance with a communication network protocol to produce an outgoing formatted secure signal; **~~and~~**

transmitting the outgoing formatted secure signal to the central computer system, wherein the central computer system is remote from the smart card communication device;

decoding, using a security device coupled to the central computer system, data from the outgoing formatted secure signal ~~and is configured~~ to detect the modification to the secured data **occurring during transmission beginning at the smart card and extending to the central computer system; ~~and to~~**

process**ing, with the central computer system,** a transaction for the smart card using the secured data included in the outgoing formatted secure signal**; and**

encoding central computer system information using the security device to produce an incoming secure data signal comprising an incoming set of secured data, the incoming set formatted to allow the smart card to detect a modification to the incoming set occurring during transmission beginning at the central computer system and extending to the smart card.

4. (Amended) A method in accordance with claim 1 further comprising the **~~steps of:~~ step of** reformatting, at the central computer system, the outgoing formatted secure signal to produce

the outgoing secure data signal, the outgoing secure data signal comprising the secured data~~;~~ ~~and~~

~~**decoding, at the central computer system**~~, **wherein the step of decoding further comprises decoding** the outgoing secure data signal to receive smart card information included within the outgoing secure data signal.

14. (Amended) A method in accordance with claim ~~13~~ **12** wherein the step of encoding further comprises the steps of:

generating a message authentication code at the central computer system; and

appending the message authentication code to the incoming data.

18. (Amended) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

exchanging secure data through a radio frequency communication channel from a smart card communication device to the smart card;

exchanging the secure data through a communication network from the central computer system to the smart card communication device;

performing a security function at the smart card on **a first set of** the secure data received from and ~~**generated**~~ **encoded by a security device** at the central computer system **for transmission to the smart card, the security function at the smart card performed** to detect whether a modification to **the first set of** the secure data occurred during transmission beginning at the central computer system and extending to the smart card;

performing the security function on the secure data **using the security device** at the central computer system to ~~**format**~~ **encode the first set of** the secure data to allow the smart card to detect a modification to **the first set of** the secure data occurring during transmission beginning at the central computer system and extending to the smart card;

decoding, using the security device, data transmitted from the smart card to detect a modification to a second set of the secure data occurring during transmission beginning at the smart card and extending to the central computer system; and

processing, using the central computer system, a transaction for the smart card using the secure data.

21. (Amended) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card, the method comprising the steps of:

downloading communication link interface software to a processor local to a smart card communication device from a HTTP server in a remote computer system;

exchanging secure data between the smart card and the smart card communication device through a radio frequency communication channel**, ~~the secure data formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system~~**;

exchanging the secure data between the smart card communication device and the central computer system through the processor running the downloaded communication link interface software, wherein the processor is coupled to the central computer system through a communication network and the processor is located remotely from the central computer system; **~~and~~**

decoding, using a security device coupled to the central computer system, a first set of the secure data received through the communication network to detect whether modification to the first set occurred during transmission beginning at the smart card and extending to the central computer system;

processing, using the central computer system, a transaction for the smart card using the secure data**; and**

encoding central computer system information using the security device to produce a second set of the secure data, the second set formatted to allow the smart card to detect a modification to the incoming set occurring during transmission beginning at the central computer system and extending to the smart card.

22. (Amended) A method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card communication device, the method comprising the steps of:

exchanging secure data with a smart card communication device through a baseband data channel, wherein the secure data comprises data exchanged between the smart card communication device and the smart card through a radio frequency channel;

formatting the secure data at the smart card communication device in accordance with a communication network protocol;

exchanging the secure data between the smart card communication device and the central computer system through a communication network, wherein **a first set of** the secure data is formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system; ~~and~~

decoding, using a security device coupled to the central computer system, a first set of the secure data received through the communication network to detect whether modification to the first set occurred during transmission beginning at the smart card and extending to the central computer system;

processing, using the central computer system, a transaction for the smart card using the secure data**; and**

encoding central computer system information using the security device to produce a second set of secured data, the second set formatted to allow the smart card to detect a modification to the second set occurring during transmission beginning at the central computer system and extending to the smart card.

25. (Amended) A smart card communication system for establishing a secure communication link between a smart card and a central computer system, the smart card communication system comprising:

a smart card communication device comprising a radio frequency transceiver adapted to exchange secure data with the smart card through a radio frequency communication channel and a data communication interface;

a processor coupled to the smart card communication device, the processor adapted to exchange the secure data with the data communication interface through a baseband data channel;

a communication network coupled to the processor and adapted to exchange the secure data in accordance with a communication network protocol between the processor and the central computer system located remotely from the processor;

a security device coupled to the central computer system and configured to**:**

decode a first set of the secure data received through the communication network to detect whether modification to the first set occurred during transmission beginning at the smart card and extending to the central computer system; and

~~format~~ **encode central computer system information to produce a second set of the secure data,** the **second set of the** secure data **formatted** to allow the smart card to detect a modification to the secure data occurring during transmission beginning at the central computer system and extending to the smart card, the security device located remotely from the processor; and

a smart card adapted to receive the **second set of the** secure data and detect whether a modification to the secure data occurred during transmission beginning at the central computer system and extending to the smart card.

29. (Amended) A smart card communication ~~device for interfacing within a smart card communication~~ system **including a smart card communication device** having a local processor coupled to a remotely located central computer system through a communication network, the **system comprising:**

a smart card communication device comprising:

a radio frequency transceiver adapted to exchange secure data with a smart card through a radio frequency communication channel, ~~the secure data formatted by the smart card to allow the central computer system to detect a modification to the secure data occurring during transmission beginning at the smart card and extending to the central computer system~~; **and**

a data communication interface adapted to exchange the secure data with the processor through a baseband data communication channel without deciphering the secure data**; and** the central computer system coupled to a security device configured to**:**

decode a first set of the secure data received through the communication network to detect whether modification to the first set occurred during transmission beginning at the smart card and extending to the central computer system; and

encode central computer system information to produce a second set of the secure data, the second set of the secure data formatted to allow the smart card to detect a modification to the secure data occurring during transmission beginning at the central computer system and extending to the smart card, the security device located remotely from the processor.

30. (Amended) A ~~device~~ **system** in accordance with claim 29 wherein the transceiver comprises:

a receiver adapted to receiving a secure outgoing radio frequency signal from a smart card to produce a secure outgoing data signal, the data communication interface adapted to send the outgoing data signal **including the first set** through the baseband data channel in a secure state.

31. (Amended) A ~~device~~ **system** in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to produce the secure outgoing data signal, the secure outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to an intelligible message only when subjected to a security function.

32. (Amended) A ~~device~~ **system** in accordance with claim 30 wherein the receiver comprises a demodulator adapted to demodulate the secure outgoing radio frequency signal to produce the secure outgoing data signal, the secure outgoing data signal comprising a plurality of logic highs and a plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

33. (Amended) A ~~device~~ **system** in accordance with claim 29 wherein the transceiver comprises a transmitter adapted to transmit a secure incoming radio frequency signal to the smart card, the secure incoming radio frequency signal based on a secure incoming data signal **including the second set** received by the data communication interface.

34. (Amended) A ~~device~~ **system** in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality of logic highs and plurality of logic lows corresponding to an intelligible message when subjected to a security function.

35. (Amended) A ~~device~~ **system** in accordance with claim 33, wherein the transmitter comprises a modulator adapted to modulate the secure incoming data signal to produce the secure incoming radio frequency signal, the secure incoming data signal comprising a plurality

of logic highs and plurality of logic lows corresponding to a verifiable authentic message only when subjected to a security function.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PRAMILA PARTHASARATHY whose telephone number is (571)272-3866. The examiner can normally be reached on 8:00a.m. to 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Pramila Parthasarathy/
Primary Examiner, Art Unit 2136
August 24, 2008